Subnormality in Group Theory

Swayam Chube

December 30, 2024

Contents

§1 Sylow Theory

§§ The Three Theorems

In this section, we shall state and prove the three Sylow theorems.

Theorem 1.1 (Sylow's First Theorem). Let G be a finite group and p be a prime dividing the order of G with $k \in \mathbb{N}$ such that $p^k \| |G|$. Then, there is a subgroup $P \leqslant G$ with $|P| = p^k$.

We denote the set of all p-Sylow subgroups by $\mathrm{Syl}_p(G)$.

Theorem 1.2 (Sylow's Second Theorem). Let G be a finite group and p be a prime dividing the order of G. Then, all subgroups in $\mathrm{Syl}_p(G)$ are conjugate.

In order to prove the above theorem, we require the following lemmas:

LEMMA 1.3. Let G be a finite group, p a prime dividing $|G|$ and $P \in \mathrm{Syl}_p(G)$. If H is a p-group contained in $N_G(P)$, then H is contained in P.

LEMMA 1.4. Let G be a finite group, p a prime dividing $|G|$, H a p-subgroup and $P \in \mathrm{Syl}_p(G)$. Then, there is $x \in G$ such that $xHx^{-1} \subseteq P$.

THEOREM 1.5 (SYLOW'S THIRD THEOREM). Let G be a finite grouop and p a prime dividing $|G|$. Let n_p be the cardinality of $\mathrm{Syl}_p(G)$. Then,

1. $n_p = |G|/|N_G(P)|$ for any $P \in \mathrm{Syl}_p(G)$
2. $n_p \mid |G|$
3. $n_p \equiv 1 \pmod p$

§§ Some Related Results

Henceforth, unless specified otherwise, G is a finite group and p is a prime dividing the order of G.

LEMMA 1.6. Let G be a finite group and P be a p-subgroup of G. Then, there is a p-Sylow subgroup of G containing P.

Proof. Choose any $Q \in \mathrm{Syl}_p(G)$. Using Lemma 1.4, there is $x \in G$ such that $xPx^{-1} \subseteq Q$, and equivalently, $P \subseteq x^{-1}Qx$, which is also a p-Sylow subgroup. This completes the proof. ■

COROLLARY 1.7. Let G be a finite group and H a subgroup. If $P \in \mathrm{Syl}_p(H)$, then there is $Q \in \mathrm{Syl}_p(G)$ such that $P = H \cap Q$.

Proof. Since P is a p-subgroup of G, due to Lemma 1.6, there is a p-Sylow subgroup Q containing it. We shall show that $P = H \cap Q$. Obviously, $P \subseteq H \cap Q$, therefore, $v_p(|H \cap Q|) \geqslant v_p(|P|) = v_p(H)$. But since $H \cap Q$ is a subgroup of H, we must have $v_p(|H|) \geqslant v_p(|H \cap Q|)$, as a result, $v_p(|H|) = v_p(|H \cap Q|)$ and $P = H \cap Q$, since $H \cap Q$ is a p-group owing the fact that it is a subgroup of Q. ■

THEOREM 1.8. Let $P \in \mathrm{Syl}_p(G)$ and H be a subgroup of G such that $N_G(P) \subseteq H$. Then, $N_G(H) = H$ and $[G : H] \equiv 1 \pmod p$.

Proof. Let $x \in N_G(H)$. Then, $P^x \subseteq H$ and is also an element of $\mathrm{Syl}_p(H)$. Using Theorem 1.2, there is $h \in H$ such that $P^x = P^h$, equivalently, $x^{-1}h \in N_G(P) \subseteq H$, implying that $x \in H$.

Now, we have

$$[G : H] = \frac{[G : N_G(P)]}{[H : N_G(P)]} = \frac{n_p(G)}{n_p(H)} \equiv 1 \pmod p$$

■

In particular, we have the following attractive result:

COROLLARY 1.9. Let $P \in \mathrm{Syl}_p(G)$. Then, $N_G(N_G(P)) = N_G(P)$.

THEOREM 1.10 (FRATTINI ARGUMENT). Let N be a normal subgroup of G and $P \in \mathrm{Syl}_p(N)$, then $G = N_G(P)N$.

Proof. Let $g \in G$. Since $N \trianglelefteq G$, $P^g \subseteq N^g \subseteq N$, $P^g \in \mathrm{Syl}_p(N)$, as a result, there is $n \in N$ such that $(P^g) = P^n$, equivalently, $P^{n^{-1}g} = P$. This immediately implies $n^{-1}g \in N_G(P)$, therefore, $g \in NN_G(P) = N_G(P)N$, completing the proof. ∎

§2 NILPOTENT GROUPS

DEFINITION 2.1 (NILPOTENT GROUPS). A group G is said to be *nilpotent* if there is a finite collection of normal subgroups $H_0, \dots, H_n$ with

$$1 = H_0 \subseteq H_1 \subseteq \cdots \subseteq H_n = G$$

and such that

$$H_{i+1}/H_i \subseteq Z(G/H_i)$$

for $0 \leqslant i < n$.

The Upper Central Series and the Lower Central Series are often useful in the analysis of nilpotent groups.

DEFINITION 2.2 (UPPER CENTRAL SERIES). For any group G, define the *Upper Central Series* as a sequence of groups,

$$1 = Z_0 \trianglelefteq Z_1 \trianglelefteq \cdots$$

such that

1. Each Z_i is characteristic in G
2. $Z_{i+1}/Z_i = Z(G/Z_i)$

DEFINITION 2.3 (LOWER CENTRAL SERIES). For any group G, define the *Lower Central Series* as a sequence of groups,

$$G = G_0 \trianglerighteq G_1 \trianglerighteq \cdots$$

such that $G_{i+1} = [G, G_i]$

§§ Analyzing The Upper And Lower Central Series

LEMMA 2.4. For all $i \geqslant 0$, let $\pi_i : G \twoheadrightarrow G/Z_i$ denote the projection. Then, $Z_{i+1} = \pi_i^{-1}(Z(G/Z_i))$.

Proof. Obvious. ∎

LEMMA 2.5. For all $i \geqslant 0$, Z_i is characteristic in G

Proof. We shall show this by induction on i. The statement is obviously true for $Z_0 = \{1\}$. Suppose we have shown that the statement holds up to $i \geqslant 0$. Let $\varphi : G \to G$ be an automorphism of groups. We now have the following commutative diagram:

$$\begin{tikzcd}
G \arrow[r, "\varphi"] \arrow[d, two heads, "\pi_i"'] \arrow[dr, dotted, "f"] & G \arrow[d, two heads, "\pi_i"] \\
G/Z_i \arrow[r, dotted, "\exists!\ \psi"'] & G/Z_i
\end{tikzcd}$$

Since $\ker \pi_i \circ \varphi = \varphi^{-1}(\ker \pi_i) = Z_i$, due to the **universal property** of the quotient, there is a unique homomorphism $\varphi : G/Z_i \to G/Z_i$ such that the above diagram commutes. Define $f = \pi_i \circ \varphi$. Then, $Z_i = \ker f = \pi_i^{-1}(\ker \psi)$, and thus, $\ker \psi = 1$. This implies that ψ is injective. Further, since π_i is surjective, so is $f = \pi_i \circ \varphi$, implying that ψ must be surjective. As a result, ψ is an automorphism of groups.

Let $g \in Z_{i+1}$, then $\pi_i(\varphi(g)) = \psi(\pi_i(g))$. We know, due to Lemma 2.4, that $\pi(g) \in Z(G/Z_i)$ and therefore, $\psi(\pi_i(g)) \in Z(G/Z_i)$, consequently $\pi_i(\varphi(g)) \in Z(G/Z_i)$ and thus, $\varphi(g) \in Z_{i+1}$.

Since we have shown for all automorphisms $\varphi : G \to G$, that $\varphi(Z_{i+1}) \subseteq Z_{i+1}$, then $\varphi^{-1}(Z_{i+1}) \subseteq Z_{i+1}$. This immediately gives us that $\varphi(Z_{i+1}) = Z_{i+1}$ for all automorphisms $\varphi : G \to G$ and Z_{i+1} is characteristic. ■

LEMMA 2.6. For all $i \geqslant 0$, we have $[G, Z_{i+1}] \subseteq Z_i$.

Proof. Let $g \in G$ and $x \in Z_{i+1}$. Let $\pi_i : G \to G/Z_i$ be the natural projection. Then,

$$\pi_i([g,x]) = [\pi_i(g), \pi_i(x)] = 1$$

where the last equality follows from the fact that $\pi_i(x) \in \pi_i(Z_{i+1}) = Z(G/Z_i)$. This immediately implies that $[g,x] \in Z_i$ and the desired conclusion. ■

LEMMA 2.7. For all $i \geqslant 0$, G_i is characteristic in G.

Proof. We shall show this by induction on i. The base case with $G_0 = G$ is trivial. Let $\varphi : G \to G$ be an automorphism of groups. Then, for all $g \in G$ and $x \in G_i$, it is not hard to see that $\varphi([g,x]) = [\varphi(g), \varphi(x)] \in [G, G_i] = G_{i+1}$. Therefore, for all automorphisms $\varphi : G \to G$, $\varphi(G_{i+1}) \subseteq G_{i+1}$. This implies that $\varphi(G_{i+1}) = G_{i+1}$, and completes the induction. ■

LEMMA 2.8. For all $i \geqslant 0$, $G_i/G_{i+1} \subseteq Z(G/G_{i+1})$.

Proof. Let $\pi_{i+1} : G \to G/G_{i+1}$ denote the natural projection. Let $x \in G_i$ and $g \in G$, then

$$1 = \pi_{i+1}([x,g]) = [\pi_{i+1}(x), \pi_{i+1}(g)]$$

since π_{i+1} is surjective, $\pi_{i+1}(x) \in Z(G/G_{i+1})$. This completes the proof. ■

THEOREM 2.9. For a group G, the following are equivalent,

1. For some $n \geqslant 0$, $Z_n = G$
2. For some $m \geqslant 0$, $G_m = 1$
3. G is nilpotent

Proof. We shall show that (1) $\implies$ (2) $\implies$ (3) $\implies$ (1), which would imply the desired conclusion.

- <u>(1) $\implies$ (2)</u> : We have a finite series

  $$1 = Z_0 \subseteq Z_1 \subseteq \cdots \subseteq Z_n = G$$

  We shall show, through induction on i, that $G_i \subseteq Z_{n-i}$. The base case with $i = 0$ is obviously true. Using Lemma 2.6, we have, for all $i \leqslant n-1$,

  $$G_{i+1} = [G, G_i] \subseteq [G, Z_{n-i}] \subseteq [G, Z_{n-i-1}] \subseteq Z_{i+1}$$

  which completes the induction. Finally, we have $G_n \subseteq Z_0 = 1$, implying the desired conclusion.

- <u>(2) $\implies$ (3)</u> : Simply define $H_i = G_{n-i}$ for all $0 \leqslant i \leqslant n$. Due to Lemma 2.8, we have that $H_{i+1}/H_i \subseteq Z(G/H_i)$.

- <u>(3) $\implies$ (1)</u> : We shall show that for all $i \geqslant 0$, $H_i \subseteq Z_i$. The base case with $i = 0$ is trivial. Consider the following commutative diagram:

  $$\begin{tikzcd} G \arrow[r, two heads, "\pi_i"] \arrow[d, two heads, "\pi'_i"'] & G/Z_i \\ G/H_i \arrow[ur, dotted, two heads, "\exists!\ \phi"'] & \end{tikzcd}$$

  Since $H_i \subseteq Z_i$, using the universal property of the quotient, there is an epimorphism $\phi : G/H_i \to G/Z_i$ such that the above diagram commutes. Let $x \in H_{i+1}$. Then, $\pi'_i(x) \in Z(G/H_i)$, therefore, for all $g \in G$

  $$1 = \phi\left(\pi'_i([g, x])\right) = \pi_i([g, x]) = [\pi_i(g), \pi_i(x)]$$

  Now, since π_i is surjective, $\pi_i(x) \in Z(G/Z_i)$, and thus, $x \in Z_{i+1}$. This implies the desired conclusion.

∎

§§ Related Results for Nilpotent Groups

LEMMA 2.10. Every finite p-group is nilpotent.

Proof. Let G be a finite p-group. We shall show that the upper central series is finite by showing the proper containment $Z_i \subsetneq Z_{i+1}$ whenever $Z_i \subsetneq G$ which would imply the desired conclusion. Let $\pi_i : G \to G/Z_i$ denote then natural projection. We know, due to Lemma 2.4, that $Z_{i+1} = \pi_i^{-1}(Z(G/Z_i))$ and since G/Z_i is a non-trivial p-group, it must have a non-trivial center, therefore, $Z_i \subsetneq Z_{i+1}$. This completes the proof. ∎

LEMMA 2.11. Let G be a nilpotent group and H, a proper subgroup of G. Then, $H \subsetneq N_G(H)$.
Note that finiteness of G is <u>*NOT*</u> *required.*

Proof. Since G is nilpotent, the upper central series $1 = Z_0 \subseteq Z_1 \subseteq \cdots \subseteq Z_n = G$ is strictly increasing (with respect to containment). Let k be the maximal index such that $Z_k \subseteq H$, that is to say, $Z_{k+1} \subsetneq H$. Now, using Lemma 2.6,

$$[Z_{k+1}, H] \subseteq [Z_{k+1}, G] \subseteq Z_k \subseteq H$$

as a result, $Z_{k+1} \subseteq N_G(H)$ which completes the proof. ∎

LEMMA 2.12. Let G be a finite nilpotent group. For every prime p dividing the order of G, the p-Sylow subgroup P is normal and therefore unique.

Proof. Recall from the study of Sylow subgroups that $N_G(N_G(P)) = N_G(P)$. This combined with Lemma 2.11 implies that $N_G(P) = G$, and P is normal in G which immediately implies uniqueness. ∎

LEMMA 2.13. Let $G_1, \ldots, G_n$ be nilpotent groups. Then, their direct product $G_1 \times \cdots \times G_n$ is also nilpotent.

Proof. The central series of the product is the pointwise product of the individual central series. ∎

THEOREM 2.14. A finite group is nilpotent if and only if it is a direct product of p-groups.

Proof. Suppose G is a finite nilpotent group, then due to Lemma 2.12, the Sylow subgroups of G are normal and it is well known that in this case, G is the direct product of the Sylow subgroups.

Conversely, if G is the direct product of p-groups, then using Lemma 2.13 and Lemma 2.10, we have that G is nilpotent. ∎

PROPOSITION 2.15. Let G be a finite group. If $H \subsetneq N_G(H)$ for every proper subgroup H of G, then G is nilpotent.

Proof. Let P be a Sylow subgroup of G. Since $N_G(P) = N_G(N_G(P))$, we must have that $N_G(P) = G$, consequently, P is normal in G. It follows that G is a (internal) direct product of its Sylow subgroups, i.e., a direct product of p-groups, each of which is nilpotent. Hence, G is nilpotent. ∎

THEOREM 2.16. Every subgroup and quotient of a nilpotent group is nilpotent.

Proof. Let G be a nilpotent group and H a subgroup of G. Let $H_0 \supseteq H_1 \supseteq \cdots$ be the lower central series of H. We shall show by induction on i, that $H_i \subseteq G_i$. The base case with $i = 0$ is trivial. We now have

$$H_{i+1} = [H, H_i] \subseteq [G, H_i] \subseteq [G, G_i] = G_{i+1}$$

this completes the induction. Finally, since the lower central series of G is finite, the lower central series of H must be finite too, implying that H is nilpotent.

On the other hand, let N be a normal subgroup of G and $G' = G/N$. Let $\pi : G \to G'$ denote the natural projection. We shall show by induction on i that $G'_i = \pi(G_i)$. The base case with $i = 0$ is trivial. We have

$$G'_{i+1} = [G', G'_i] = \pi([G, G_i]) = \pi(G_{i+1})$$

This completes the induction and implies that the lower central series of G' is finite. ■

LEMMA 2.17. A group G is nilpotent if and only if $G/Z(G)$ is nilpotent.

Proof. One direction of the statement is trivial due to Theorem 2.16. Now suppose $\widetilde{G} = G/Z(G)$ is nilpotent and let $\pi : G \to G/Z(G)$ denote the natural projection. Let $\widetilde{G} = \widetilde{G}_0 \supseteq \widetilde{G}_1 \supseteq \cdots \supseteq \widetilde{G}_n = 1$ denote the lower central series of $\widetilde{G}$. We shall show by induction on i that $G_i \subseteq \pi^{-1}(\widetilde{G}_i)$. We have

$$\pi(G_{i+1}) = \pi([G, G_i]) = [\pi(G), \pi(G_i)] \subseteq [\widetilde{G}, \widetilde{G}_i] = \widetilde{G}_{i+1}$$

This completes the induction and implies the desired conclusion. ■

LEMMA 2.18. Let G be a nilpotent group and N a non-trivial normal subgroup of G. Then, $Z(G) \cap N$ is non-trivial.

Proof. Let $1 = Z_0 \subseteq Z_1 \subseteq \cdots \subseteq Z_n = G$ denote the upper central series of G. Let k be the unique index such that $Z_k \cap N = 1$ while $Z_{k+1} \cap N \neq 1$. We shall show that $G \cap Z_{k+1} \subseteq Z(G)$. Indeed, we have

$$[G, N \cap Z_{k+1}] \subseteq [G, N] \cap [G, Z_{k+1}] \subseteq N \cap Z_k = 1$$

where we used that for all normal subgroups N, $[G, N] \subseteq N$ and Lemma 2.6.

Since $[G, N \cap Z_{k+1}] = 1$, we must have that $1 \neq N \cap Z_{k+1} \subseteq Z(G)$, which completes the proof. ■

§§ The Fitting Subgroup

DEFINITION 2.19. Let G be a finite group. For every prime p, let $\mathrm{Syl}_p(G)$ denote the collection of all Sylow p-subgroups of G. Define

$$\mathbf{O}(G) = \bigcap_{H \in \mathrm{Syl}_p(G)} H.$$

Since all Sylow p-subgroups of G are conjugate, $\mathbf{O}(G)$ is a normal p-subgroup of G. For distinct primes $p \neq q$, $\mathbf{O}_p(G) \cap \mathbf{O}_q(G) = \{1\}$ and hence, $\mathbf{O}_p(G)$ commutes with $\mathbf{O}_q(G)$.

PROPOSITION 2.20. $\mathbf{O}_p(G)$ contains every normal p-subgroup of G.

Proof. Let $P \trianglelefteq G$ be a normal p-subgroup. It is well-known that there is a Sylow p-subgroup of G containing P. But since all the Sylow p-subgroups of G are conjugate, P must be contained in all of them, and hence, in $\mathbf{O}_p(G)$. ■

Consider the product map

$$\mu : \prod_{p \mid G} \mathbf{O}_p(G) \longrightarrow G,$$

given by $\mu\left((x_p)\right) = \prod x_p$. We contend that this map is injective. Let H be the image of μ. Since each $\mathbf{O}_p(G)$ is contained in H, their orders must divide the order of H. Further, since they are coprime, we have that the order of H is equal to the order of the product $\prod_p \mathbf{O}_p(G)$ and hence, the map must be injective.

DEFINITION 2.21. The image of μ is denoted by $\mathbf{F}(G)$ and is called the *Fitting subgroup*.

PROPOSITION 2.22. $\mathbf{F}(G)$ is a normal nilpotent subgroup of G. Further, it contains every nilpotent normal subgroup of G.

Proof. Being a product of normal subgroups, $\mathbf{F}(G)$ is normal. It is nilpotent as it is isomorphic to a direct product of p-groups, each of which is nilpotent.

Let $N \trianglelefteq G$ be a normal nilpotent subgroup of G and suppose $P \in \mathrm{Syl}_p(N)$. Then, P is normal in G. For any $g \in G$, P^g is also contained in N (owing to N being normal in G) and has the same cardinality as P, i.e. is a Sylow p-subgroup of N. Consequently, $P = P^g$ and P is normal in G, whence P is contained in $\mathbf{O}_p(G) \subseteq \mathbf{F}(G)$. This shows that all Sylow subgroups of N are contained in $\mathbf{F}(G)$. Since N is the product of its Sylow subgroups, we have shown that N is contained in $\mathbf{F}(G)$. ■

PROPOSITION 2.23. $\mathbf{F}(G)$ is characteristic in G.

Proof. Let $\varphi \in \mathrm{Aut}(G)$. Note that $\varphi(\mathbf{F}(G))$ is also nilpotent and normal in G. Consequently, it must be contained in $\mathbf{F}(G)$, whence the conclusion follows. ■

PROPOSITION 2.24. If $N \trianglelefteq G$, then $\mathbf{F}(N) \subseteq \mathbf{F}(G)$.

Proof. We know that $\mathbf{F}(N)$ is nilpotent and hence, it suffices to show that it is normal in G. For any $g \in G$, the map $x \mapsto g^{-1}xg = x^g$ is an automorphism of N. Since $\mathbf{F}(N)$ is characteristic in N, we have that $\mathbf{F}(N)^g \subseteq \mathbf{F}(N)$, whence the conclusion follows. ■

§3 Solvable Groups

Definition 3.1 (Derived Series). Let G be a group. The *derived series* of a group is given by the sequence of subgroups

$$G = G^{(0)} \supseteq G^{(1)} \supseteq \cdots$$

such that $G^{(i+1)} = [G^{(i)}, G^{(i)}]$.

Definition 3.2 (Solvable Groups). A group G is said to be solvable if there is $n \geqslant 0$ and a series $G = H^{(0)} \supseteq H^{(1)} \supseteq \cdots H^{(n)} = 1$ such that for all $0 \leqslant i \leqslant n-1$, each $H^{(i+1)}$ is normal in $H^{(i)}$ and $H^{(i)}/H^{(i+1)}$ is Abelian.

§§ Analyzing the Derived Series

Lemma 3.3. For all $i \geqslant 0$, $G^{(i)}$ is characteristic in G.

Proof. We shall show this statement by induction on i. The base case with $i = 0$ is trivial. Let $\varphi : G \to G$ be an automorphism of groups. Then,

$$\varphi(G^{(i+1)}) = \varphi([G^{(i)}, G^{(i)}]) = [\varphi(G^{(i)}), \varphi(G^{(i)})] = G^{(i+1)}$$

■

Theorem 3.4. For any group G, the following are equivalent

1. There is $n \geqslant 0$ such that $G^{(n)} = 1$
2. G is solvable

Proof.

- $\underline{(1) \implies (2):}$ Simply choose $H^{(i)} = G^{(i)}$.
- $\underline{(2) \implies (1):}$ We shall show by induction on i that $G^{(i)} \subseteq H^{(i)}$. The base case with $i = 0$ is trivial. Now, for all $0 \leqslant i \leqslant n-1$,

  $$G^{(i+1)} = [G^{(i)}, G^{(i)}] \subseteq [H^{(i)}, H^{(i)}] \subseteq H^{(i+1)}$$

  where the last containment follows from the fact that $H^{(i)}/H^{(i+1)}$ is Abelian. This completes the proof.

■

Lemma 3.5. All nilpotent groups are solvable.

Proof. Let $G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_n = 1$ be the lower central series. We shall show by induction on i that for all $0 \leqslant i \leqslant n$, $G^{(i)} \subseteq G_i$. The base case with $i = 0$ is trivial. For $i \geqslant 0$, we have

$$G^{(i+1)} = [G^{(i)}, G^{(i)}] \subseteq [G_i, G_i] \subseteq [G, G_i] = G_{i+1}$$

This completes the induction step and implies the desired conclusion. ■

COROLLARY 3.6. All p-groups are solvable.

THEOREM 3.7. Let $1 \to N \xrightarrow{\alpha} G \xrightarrow{\pi} H \to 1$ be a short exact sequence. Then, G is solvable if and only if both N and H are solvable.

Proof. Without loss of generality, we may assume N to be a normal subgroup in G and H its corresponding quotient.

Suppose G is solvable. Then, we can inductively show that $N^{(i)} \subseteq G^{(i)}$, implying the solvability of $N^{(i)}$. On the other hand, $\pi(G^{(i)}) = H^{(i)}$, again implying the solvability of H.

Conversely, suppose both N and H are solvable. Then, $\pi(G^{(n)}) = 1$ for some $n \geqslant 0$, therefore, $G^{(n)} \subseteq N$. From here, it isn't hard to show that $G^{(n+i)} \subseteq N^{(i)}$, implying the solvability of G. This completes the proof. ■

COROLLARY 3.8. Let G be a solvable group. If H is a subgroup of G, then H is solvable.

PROPOSITION 3.9. A minimal normal subgroup of a solvable group is an elementary abelian p-group.

§§ Two theorems of P. Hall

THEOREM 3.10 (HALL). Let G be a solvable group of order $|G| = ab$, where $\gcd(a,b) = 1$.

Existence: G admits a subgroup of order a.

Conjugacy: Any two subgroups of order a are conjugate in G.

Proof. Induct on $|G|$. The base cases where $|G|$ is a prime number are trivially established.
Case 1. G contains a non-trivial normal subgroup H of order $a'b'$, where $a' \mid a$, $b' \mid b$, and $b' < b$.
Existence. In this case, G/H is a solvable group of order group of order $(a/a')(b/b') < ab$. Due to the induction hypothesis, G/H admits a subgroup A/H of order a/a', where A is a subgroup of G of order $ab' < ab$. Since A is solvable, the induction hypothesis applies to A, which then admits a subgroup of order a.
Conjugacy. Let A and A' be subgroups of G of order a. Note that AH is a subgroup of G of order

$$|AH| = \frac{|A||H|}{|A \cap H|} \leqslant |A|\frac{|H|}{|A \cap H|}.$$

Note that $|A \cap H|$ divides $|H| = a'b'$ and since $\gcd(a', b') = 1$ and $|A \cap H|$ divides $|A| = a$, we see that $|H|/|A \cap H| \leqslant b'$. It follows that $|AH| \leqslant ab'$. But, on the other hand, AH contains A and H as subgroups, whence $a \mid |AH|$ and $a'b' \mid |AH|$, whence $ab' \mid |AH|$, that is, $|AH| = ab'$. Similarly, one can argue that $|A'H| = ab'$.

Now, $|G/H| = a/a' \cdot b/b'$ and $|AH/H| = |A'H/H| = a/a'$. The induction hypothesis applies and these groups are conjugate in G/H, whence AH and $A'H$ are conjugate in G. That is, there is an $x \in G$ such that $xAHx^{-1} = A'H$. Therefore, xAx^{-1} and A' are subgroups of $A'H$ of order a, and since $|A'H| < |G|$, the induction hypothesis applies once again, and A nad A' are conjugate in G.

It follows from the first case that if there is a non-trivial proper normal subgroup whose order is not divisible by b, then the theorem has been proved. We may therefore assume that $b \mid |H|$ for every non-trivial normal subgroup H of G. If H is a minimal normal subgroup of G, then due to Proposition 3.9, H is an elementary abelian p-group. It follows that $b = p^m = |H|$ for some $m \geqslant 1$. Thus, H is a normal (hence unique) Sylow p-subgroup of G. So we have shown that every minimal normal subgroup of G is the Sylow p-subgroup, and hence, G admits a unique minimal normal subgroup. The problem is no reduced to the following:

$\boxed{\textit{Case 2.}}$ $|G| = ap^m$, where $p \nmid a$, and G has a normal abelian Sylow p-subgroup H, and H is the unique minimal normal subgroup in G.

Existence. The group G/H is solvable of order a. If K/H is a minimal normal subgroup of G/H, then $|K/H| = q^n$ for some prime $q \neq p$ due to Proposition 3.9; and so $|K| = p^m q^n$, also note that $K \trianglelefteqslant G$. If Q is a Sylow q-subgroup of K, then $K = HQ$. Let $N^* = N_G(Q)$ and let $N = N^* \cap K = N_K(Q)$. Then Theorem 1.10 gives $G = KN^*$. Since

$$G/K \cong KN^*/K \cong N^*/N^* \cap K = N^*/N,$$

we have $|N^*| = |G||N|/|K|$. But $K = HQ$, and $Q \subseteq N \subseteq K$ gives $K = HN$, whence $|K| = |HN| = |H||N|/|H \cap N|$, so that

$$|N^*| = \frac{|G||N|}{|K|} = \frac{|G||N||H \cap N|}{|H||N|} = \frac{|G|}{|H|}|H \cap N| = a|H \cap N|.$$

We claim that $H \cap N = 1$. We show this in two stages:

- First, we show that $H \cap N \subseteq Z(K)$. Let $x \in H \cap N$. Every $k \in K$ has the form $k = hs$ for some $h \in H$ and $s \in Q$. Since H is abelian, it suffices to show that x commutes commutes with s. Note that the commutator $[x, s] \in Q$, since x normalizes Q. On the other hand, $[x, s] = x(sx^{-1}s^{-}1) \in H$, because H is normal in G. Therefore, $[x, s] \in Q \cap H = 1$. Thus, $H \cap N \subseteq Z(K)$.

- Next, we show that $Z(K) = 1$. Since $Z(K)$ is characteristic in K and K is normal in G, we have that $Z(K) \trianglelefteqslant G$. If $Z(K)$ were non-trivial, then it would contain a minimal normal subgroup of G, i.e., H due to uniqueness. But since $K = HQ$, and H is central in K, we see that Q must be normal in K. A normal Sylow subgroup is characteristic (owing to its uniqueness), and hence, $Q \trianglelefteqslant G$. Again, this means $H \subseteq Q$, because Q must also contain a minimal normal subgroup of G. This is absurd, since H is a p-group. Thus, $Z(K) = 1$.

We have shown that $|N^*| = a$, thereby proving existence.

Conjugacy. Let A be another subgroup of G of order a. Since $|AK|$ is divisible by a and by $|K| = p^m q^n$, it follows that $|AK| = ap^m = |G|$, that is, $AK = G$. Hence,

$$\frac{G}{K} \cong \frac{AK}{K} \cong \frac{A}{A \cap K},$$

so $|A \cap K| = q^n$. From Sylow's theorem, $A \cap K$ is conjugate to Q. It follows that $N^* = N_G(Q)$ is conjugate to $N_G(A \cap K)$, whence $a = |N_G(A \cap K)|$. Since $A \subseteq N_G(A \cap K)$, we must have $A = N_G(A \cap K)$ and that A is conjugate to N^* as desired. ■

§4 SUBNORMALITY

DEFINITION 4.1. Let G be a grouop. A subgroup $S \subseteq G$ is said to be *subnormal* in G if there exist subgroups H_i of G such that

$$S = H_0 \trianglelefteqslant H_1 \trianglelefteqslant \cdots \trianglelefteqslant H_r = G.$$

In this situation, we write $S \lhd\!\lhd G$. The smallest integer r for which the above holds is called the *subnormal depth* of S in G.

REMARK 4.2. Note that the definition of a subnormal subgroup behaves well with respect to "contraction". That is, if $S \lhd\!\lhd G$ and H is any subgroup of G, then $S \cap H \lhd\!\lhd H$. As a result, if $S, T \lhd\!\lhd G$, then $S \cap T \lhd\!\lhd G$.

Now, suppose $\varphi : G \to \overline{G}$ is a surjective group homomorphism and $S \lhd\!\lhd G$. Then, $\varphi(S) \lhd\!\lhd \overline{G}$, since the image of a subnormal series under φ is still subnormal.

LEMMA 4.3. Let G be a finite group. Then G is nilpotent if and only if every subgroup of G is subnormal.

Proof. Suppose G is nilpotent and H is a proper subgroup of G. Define $H_0 = H$ and $H_{i+1} = N_G(H_i)$. Then, either $H_{i+1} = G$ or $H_i \subsetneq H_{i+1}$. This gives us a subnormal series for H.

Conversely, suppose every subgroup of G is subnormal and let H be a proper subgroup. There is a sequence

$$H = H_0 \lhd H_1 \lhd \cdots \lhd H_n = G.$$

In particular, we may assume that $H_i \subsetneq H_{i+1}$ for $0 \leqslant i \leqslant n-1$. Hence, $H \subsetneq H_1 \subseteq N_G(H)$. Due to Proposition 2.15, we see that G must be nilpotent. ∎

PROPOSITION 4.4. Let G be a finite group and $H \leqslant G$. Then $H \subseteq \mathbf{F}(G)$ if and only if H is nilpotent and subnormal in G.

Proof. Since $\mathbf{F}(G)$ is nilpotent, if H were contained in $\mathbf{F}(G)$, then it would be niloptent too. Further, due to the preceding lemma, $H \lhd\!\lhd G$ and $\mathbf{F}(G) \lhd G$, whence $H \lhd\!\lhd G$.

We prove the converse by induction on $|G|$. If $H = G$, then there is nothing to prove, since G would be nilpotent and $\mathbf{F}(G) = G$. Suppose now that $H \subsetneq G$. There is a subnormal series

$$H = H_0 \lhd H_1 \lhd \cdots \lhd H_n = G.$$

where every successive containment is proper. Set $M = H_{n-1} \lhd G$. The inductive hypothesis applies since H is nilpotent and subnormal in M, consequently, $H \subseteq \mathbf{F}(M) \subseteq \mathbf{F}(G)$, due to Proposition 2.24, thereby completing the proof. ∎

DEFINITION 4.5. A *minimal normal subgroup* of a group G is a non-identity normal subgroup of G that does not admit any non-trivial normal subgroups. The *socle* of a *finite* group G is defined to be the subgroup generated by all minimal normal subgroups of G, which is precisely their product.

If M and N are two minimal normal subgroups of G, then $M \cap N = \{1\}$ and hence, every element of M commutes with every element of N. Thus, $\mathrm{Soc}(G)$ is precisely the product of all minimal normal subgroups of G and is a normal subgroup of G. Further, if G is a finite group that is not trivial, then it admits a non-trivial minimal finite group, and hence, $\mathrm{Soc}(G)$ is non-trivial.

PROPOSITION 4.6. Let G be a finite group. Then $\mathrm{Soc}(G)$ is characteristic in G.

Proof. Let $\varphi \in \mathrm{Aut}(G)$. For a minimal normal subgroup M of G, $\varphi(M)$ is also a minimal normal subgroup of G. Consequently, φ permutes the minimal normal subgroups of G and thus stabilizes the socle. ■

THEOREM 4.7. Let G be a finite group, $S \lhd\!\lhd G$, and M a minimal normal subgroup of G. Then $M \subseteq N_G(S)$.

Proof. Induction on $|G|$. If $S = G$, then there is nothing to prove, so we can suppose that $S \subsetneq G$. Since $S \lhd\!\lhd G$, arguing as in the preceding proof, we can choose a normal subgroup $N \subsetneq G$ such that $S \lhd\!\lhd N \lhd G$.

If $M \cap N = 1$, then every element of M commutes with every element of N, and hence, $M \subseteq C_G(N) \subseteq C_G(S) \subseteq N_G(S)$. Suppose now that $M \cap N$ is non-trivial. But since M is a minimal normal subgroup, $M = M \cap N$, i.e. $M \subseteq N$.

The inductive hypothesis applies to N, whence every minimal normal subgroup of N normalizes S, consequently, $\mathrm{Soc}(N)$ normalizes S. Therefore, it suffices to show that $M \subseteq \mathrm{Soc}(N)$.

Since N is a finite group and M is a non-trivial normal subgroup of N, it contains a minimal normal subgroup. That is, $M \cap \mathrm{Soc}(N) \neq 1$. Since $\mathrm{Soc}(N)$ is characteristic in N, it must be normal in G. Owing to the minimality of M in G, $M \cap \mathrm{Soc}(N) = M$, that is, $M \subseteq \mathrm{Soc}(N)$ as desired. ■

THEOREM 4.8 (WIELANDT). Let G be a finite group and $S, T \lhd\!\lhd G$. Then $\langle S, T\rangle \lhd\!\lhd G$.

Proof. Induction on $|G|$. Suppose G is non-trivial, choose a minimal normal subgroup M of G and set $\overline{G} = G/M$. By abuse of notation, we use the "overbar" to denote the homomorphism $G \to \overline{G}$. Note that

$$\langle \overline{S}, \overline{T}\rangle = \overline{\langle S, T\rangle} = \overline{\langle S, T\rangle M},$$

since M is the kernel of $G \to \overline{G}$. The inductive hypothesis applies to $\overline{G}$ and hence, $\langle \overline{S}, \overline{T}\rangle \lhd\!\lhd \overline{G}$. There is a natural bijection between the subgroups of G containing M and the subgroups of $\overline{G}$, which preserves normality and hence, subnormality. Therefore, $\langle S, T\rangle M \lhd\!\lhd G$.

Finally, note that $M \subseteq N_G(S), N_G(T)$ and hence, $M \subseteq N_G(\langle S, T\rangle)$, whence $\langle S, T\rangle \lhd \langle S, T\rangle M \lhd\!\lhd G$, whence the conclusion follows. ■

LEMMA 4.9. Let G be a group and $H \leqslant G$. If $HH^x = G$ for some $x \in G$, then $H = G$.

Proof. Write $x = uv$, where $u \in H$ and $v \in H^x$. Then $xv^{-1} = u$ and we have

$$H^x = (H^x)^{v^{-1}} = H^{uv^{-1}} = H^u = H.$$

Then $G = HH^x = HH = H$, as desired. ■

THEOREM 4.10 (WIELANDT ZIPPER LEMMA). Let G be a finite group and $S \leqslant G$ such that $S \lhd\lhd H$ for every proper subgroup H of G containing S. If S is not subnormal in G, then there is a unique maximal subgroup of G containing S.

Proof. We induct on $|G : S|$. Since S is not normal, $N_G(S) \subsetneq G$, and thus $N_G(S) \subseteq M$ for some maximal subgroup M of G. We must show that this M is unique. Suppose that $S \subseteq K$ is another maximal subgroup of G. We shall show that $K = M$.

By our hypothesis, $S \lhd\lhd K$. Suppose first that $S \trianglelefteqslant K$. Then $K \subseteq N_G(S) \subseteq M$ and hence due to maximality, $K = M$, as desired. We can suppose, therefore, that S is not normal in K. Choose the shortest subnormal series

$$S = H_0 \lhd H_1 \lhd \cdots \lhd H_r = K,$$

where $r \geqslant 2$, since S is not normal in K. Also, S is not normal in H_2 since otherwise we could delete H_1 to obtain a shorter subnormal series. Let $x \in H_2$ be such that $S^x \neq S$, and write $T = \langle S, S^x \rangle \supsetneq S$. Note that $T \subseteq K$. Also, $S^x \subseteq H_1^x = H_1 \subseteq N_G(S)$, and thus, $T \subseteq N_G(S) \subseteq M$. Furthermore, we have that $S \lhd T \subsetneq G$.

Note that S^x also satisfies the hypothesis of the theorem because conjugation by x is an automorphism of G. We claim that the subgroup $T = \langle S, S^x \rangle$ also satisfies the same hypothesis. In particular, we need to show that if $T \subseteq H \subsetneq G$, then $T \lhd\lhd H$ and T is not subnormal in G.

First, if $T \subseteq H \subsetneq G$, then $S \subseteq H$, and thus $S \lhd\lhd H$, and similarly, $S^x \lhd\lhd H$, consequently, due to Theorem 4.8, $T \lhd\lhd H$. Also, $S \lhd T$ and so if $T \lhd\lhd G$, then it would follow that $S \lhd\lhd G$, a contradiction. Thus T is not subnormal in G.

Our inductivev hypothesis applies to T since it properly contains S, and hence T is contained in a unique maximal subgroup of G. But since $T \subseteq M$ and $T \subseteq K$, we have that $M = K$, as desired. ∎

DEFINITION 4.11. For a subgroup H of a group G, let H^G denote the smallest normal subgroup of G containing H. This is known as the *normal closure* of H in G.

THEOREM 4.12 (BAER). Let G be a finite group and $H \leqslant G$. Then $H \subseteq \mathbf{F}(G)$ if and only if $\langle H, H^x \rangle$ is nilpotent for all $x \in G$.

Proof. If $H \subseteq \mathbf{F}(G)$, then $H^x \subseteq \mathbf{F}(G)$ for every $x \in G$, since $\mathbf{F}(G) \trianglelefteqslant G$. Hence, $\langle H, H^x \rangle \subseteq \mathbf{F}(G)$. But since $\mathbf{F}(G)$ is nilpotent, so is $\langle H, H^x \rangle$.

Conversely, suppose $\langle H, H^x \rangle$ is nilpotent for every $x \in G$. We induct on $|G|$. Taking $x = 1$, we see that H is nilpotent, whence it suffices to prove that $H \lhd\lhd G$.

Suppose H is not subnormal in G. For any proper subgroup K of G containing H, the induction hypothesis applies to K and hence, $H \subseteq \mathbf{F}(K)$, that is, $H \lhd\lhd K$. Due to Wielandt's Zipper Lemma, there is a unique maximal subgroup M of G containing H.

If $\langle H, H^x \rangle = G$, then G is nilpotent and $\mathbf{F}(G) = G$, and $H \lhd\lhd G$, a contradiction. Thus, $\langle H, H^x \rangle \subsetneq G$ for all $x \in G$. This subgroup must be contained in a maximal subgroup of G; but since it contains H, and there is a unique maximal subgroup M containing H, we conclude that $H^x \subseteq M$ for all $x \in G$. Therefore, $H^G \subseteq M \subsetneq G$.

Since H^G is normal and properly contained in G, the induction hypothesis applies and $H \lhd\lhd H^G \lhd G$, that is, $H \lhd\lhd G$, a contradiction. This completes the proof. ∎

THEOREM 4.13 (ZENKOV). Let G be a finite group and $A, B \leqslant G$ be abelian subgroups. If M is a minimal element in the set

$$\{A \cap B^g : g \in G\},$$

then $M \subseteq \mathbf{F}(G)$.

Proof. The set $\{A \cap B^g : g \in G\}$ remains unchanged upon replacing B with B^g. Therefore, we may assume that $M = A \cap B$. We prove the statement by induction on $|G|$. First, suppose that $G = \langle A, B^g \rangle$ for some $g \in G$. Since A and B^g are abelian, we have $A \cap B^g \subseteq Z(G)$, and hence,

$$A \cap B^g = (A \cap B^g)^{g^{-1}} = A^{g^{-1}} \cap B \subseteq B.$$

It follows that $A \cap B^g \subseteq A \cap B \subseteq M$, and by the minimality of M, we have $M = A \cap B^g \subseteq Z(G) \subseteq F(G)$, as desired.

Next, assume that $\langle A, B^g \rangle \subsetneq G$ for all $g \in G$. To show that M is contained in $\mathbf{F}(G)$, it suffices to show that every Sylow p-subgroup P of M is contained in $\mathbf{F}(G)$ (because every group is generated by its Sylow subgroups). Due to Theorem 4.12, it suffices to show that $\langle P, P^g \rangle$ is nilpotent for every $g \in G$.

Fix $g \in G$, and let $H = \langle A, B^g \rangle \subsetneq G$, and $C = B \cap H$. For $h \in H$, we have

$$A \cap C^h = A \cap (B \cap H)^h = A \cap B^h \cap H = A \cap B^h.$$

In particular, $M = A \cap B = A \cap B \cap H = A \cap C$ is minimal in the set $\{A \cap C^h : h \in H\}$ since its minimal in the larger set $\{A \cap B^g : g \in G\}$. By the inductive hypothesis, $P \subseteq M \subseteq \mathbf{F}(H)$, and hence, $P \subseteq \mathbf{O}_p(H)$, since $\mathbf{O}_p(H)$ is the unique Sylow p-subgroup of $\mathbf{F}(H)$. Also, $P^g \subseteq B^g \subseteq H$, and since $\mathbf{O}_p(H)$ is a normal subgroup, we have that $\mathbf{O}_p(H)P^g$ is a p-group containing $\langle P, P^g \rangle$. In particular, $\langle P, P^g \rangle$ is a p-group, whence is nilpotent, as desired. ∎

COROLLARY 4.14. Let A be an abelian subgroup of a non-trivial finite group G, and suppose that $|A| \geqslant |G : A|$. Then $A \cap \mathbf{F}(G)$ is non-trivial.

Proof. If $A = G$, then there is nothing to prove. Suppose now that $A \subsetneq G$. If $g \in G$, then $|A||A^g| = |A|^2 \geqslant |A||G : A| = |G|$. Further, due to Lemma 4.9, $AA^g \subsetneq G$. Hence,

$$|G| > |AA^g| = \frac{|A||A|^g}{|A \cap A^g|} \geqslant \frac{|G|}{|A \cap A^g|},$$

and thus $A \cap A^g$ is non-trivial. Since this holds for all $g \in G$, we can apply Theorem 4.13 to deduce that there is a $g \in G$ such that $A \cap A^g \subseteq \mathbf{F}(G)$, whence $A \cap \mathbf{F}(G)$ is non-trivial. ∎

THEOREM 4.15 (LUCCINI). Let A be a proper cyclic subgroup of a finite group G, and let $K = \mathrm{core}_G(A)$. Then $|A : K| < |G : A|$, and in particular, if $|A| \geqslant |G : A|$, then K is non-trivial.

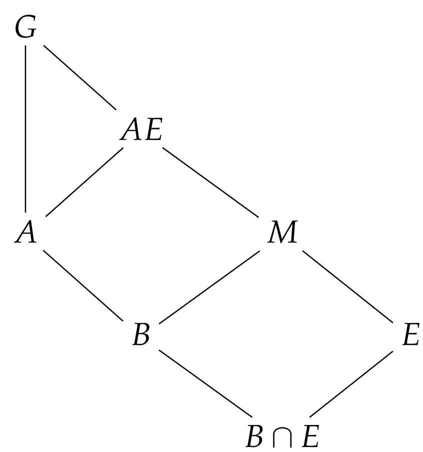
Proof. Induction on $|G|$. Note that A/K is a proper cyclic subgroup of G/K and the core of A/K in G/K is trivial. If K is non-trivial, then the inductive hypothesis applies and we deduce that

$$|A/K| = |A/K : \mathrm{core}_{G/K}(A/K)| < |G/K : A/K| = |G : A|.$$

We may now assume that $K = 1$, and we shall show that $|A| < |G : A|$. Suppose not, that is, $|A| \geqslant |G : A|$. Due to Corollary 4.14, $A \cap \mathbf{F}(G)$ is non-trivial. In particular, $\mathbf{F}(G)$ is non-trivial, so we can choose a minimal normal subgroup E of G with $E \subseteq \mathbf{F}(G)$ (since $\mathbf{F}(G)$ is normal in G). Due to Lemma 2.18, $E \cap Z(\mathbf{F}(G))$ is non-trivial; but since $Z(\mathbf{F}(G))$ is characteristic in $\mathbf{F}(G)$, it is normal in G. Due to the minimality of E, we must have $E \subseteq Z(\mathbf{F}(G))$, in particular, E is abelian. Being abelian, every Sylow subgroup of E is characteristic in G, whence due to minimality, E itself must be a p-group. We contend that E is an elementary abelian p-group. Indeed, consider $\widetilde{E} = \{x^p \colon x \in E\}$, which is proper and characteristic in E, and hence, is normal in G. Due to minimality of E, $\widetilde{E} = 1$, as desired.

Since $E \subseteq Z(\mathbf{F}(G))$, we see that E normalizes the non-trivial group $A \cap \mathbf{F}(G)$, and of course A normalizes this too. Then $A \cap \mathbf{F}(G) \trianglelefteqslant AE$. Since $\mathrm{core}_G(A) = 1$, we cannot have $AE = G$, else $A \cap \mathbf{F}(G)$ would be contained in the core. It follows that $AE \subsetneq G$.

Set $\overline{G} = G/E$, $\overline{A} = AE/E \subsetneq \overline{G}$, $\overline{M} = \mathrm{core}_{\overline{G}}(\overline{A})$, with $E \subseteq M$ and $M \trianglelefteqslant G$. Note that $M \subseteq AE$, and hence, $AE \subseteq AM \subseteq AE$, whence $AM = AE$. Due to the inductive hypothesis, we must have $|\overline{A} : \overline{M}| < |\overline{G} : \overline{A}|$, that is, $|AE : M| < |G : AE|$.



Let $B = A \cap M$ so that B is cyclic. We have

$$|AE : A| = |AM : A| = |M : A \cap M| = |M : B|,$$

and hence, $|AE : M| = |A : B|$. Therefore,

$$|M : B| = |AE : A| = \frac{|G : A|}{|G : AE|} < \frac{|G : A|}{|AE : M|} = \frac{|G : A|}{|A : B|} \leqslant \frac{|A|}{|A : B|} = |B|.$$

Before we proceed, note that $E \subseteq M \subseteq AE = EA$, and hence, because of what's colloquially known as Dedekind's rule, $M = E(A \cap M) = EB = BE$ (since $E \trianglelefteqslant G$).

Suppose M is abelian, and let $\varphi : M \to M$ be the endomorphism $\varphi(m) = m^p$. Then $E \subseteq \ker \varphi$ since it is an elementary abelian p-group. It follows that

$$\varphi(M) = \varphi(EB) = \varphi(B) \subseteq B \subseteq A.$$

Now, $M \trianglelefteqslant G$, and hence, $\varphi(M) \trianglelefteqslant G$, and we conclude that $\varphi(M) = 1$, since $\mathrm{core}_G(A) = 1$. Then $\varphi(B) = 1$, and since B is cyclic, it follows that $|B| \leqslant p$. Then $|M : B| < |B| \leqslant p$, and since $M/B \cong E/B \cap E$[1], it is a p-group, it follows that $M/B = 1$, that is, $M = B \subseteq A$. But $M \trianglelefteq G$, and since $M \subseteq A$, we have $M = 1$, whence $E = 1$, a contradiction.

It follows that M is non-abelian, and since $M/E \cong B/B \cap E$ is cyclic, we conclude that E is not central in M[2], and so $E \cap Z(M) \subsetneq E$. Again recall that $Z(M)$ is characteristic in M and hence normal in G. Due to the minimality of E, we must have $E \cap Z(M) = 1$, and thus $Z(M)$ is cyclic because the restriction of the surjection $M \twoheadrightarrow M/E$ is injective on $Z(M)$.

Since B is an abelian subgroup of M and $|M : B| < |B|$, due to Corollary 4.14, we have that $B \cap \mathbf{F}(M)$ is non-trivial. Due to Proposition 2.24, $\mathbf{F}(M) \subseteq \mathbf{F}(G)$, and so E centralizes $\mathbf{F}(M)$ because $E \subseteq Z(\mathbf{F}(G))$. Since every element of $B \cap \mathbf{F}(M)$ commutes with every element of B (since B is abelian) and every element of E, we see that $B \cap \mathbf{F}(M)$ is a non-trivial central subgroup of $EB = M$. Since $Z(M)$ is cyclic, we see that $B \cap \mathbf{F}(M) \subseteq Z(M)$ is characteristic in $Z(M) \trianglelefteq G$[3], and hence, $B \cap \mathbf{F}(M)$ is a non-trivial normal subgroup of G contained in A, a contradiction. This completes the proof. ■

THEOREM 4.16 (HOROSEVSKII). Let $\sigma \in \mathrm{Aut}(G)$, where G is a non-trivial finite group. Then the order $o(\sigma)$ of σ as an element of $\mathrm{Aut}(G)$ is strictly smaller than $|G|$.

Proof. Let $A = \langle \sigma \rangle \subseteq \mathrm{Aut}(G)$, so that A is a cyclic group of order equal to the order of σ as an element of $\mathrm{Aut}(G)$. Set $\Gamma = G \rtimes_\theta A$, where $\theta : A \to \mathrm{Aut}(G)$ is the obvious inclusion map. We identify G and A with subgroups $G \times \{1\}$ and $\{1\} \times A$ of Γ. Note that the conjugation action of A on G as elements of Γ is given by $g^\tau = \tau(g) \in G$ for $\tau \in A$. By definition of an automorphism, every non-identity element of A acts non-trivially on G, and hence, $A \cap C_\Gamma(G) = 1$.

Since G is non-trivial and A is cyclic, due to Theorem 4.15, $|A : K| < |\Gamma : A|$, where $K = \mathrm{core}_\Gamma(A)$. But then $K \cap G \subseteq A \cap G = 1$, and both K and G are normal in Γ, consequently, their elements commute, that is, $K \subseteq C_\Gamma(G)$. Since $K \subseteq A$, we see that $K \subseteq A \cap C_\Gamma(G) = 1$, that is, K is trivial. Thus,

$$o(\sigma) = |A| = |A : K| < |\Gamma : A| = G,$$

as desired. ■

---

[1]These quotients make sense because M is abelian.
[2]Recall that if $G/Z(G)$ is cyclic, then G is abelian.
[3]Every subgroup of a cyclic group is characteristic.